PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-103425
(43)Date of publication of application : 15.04.1994

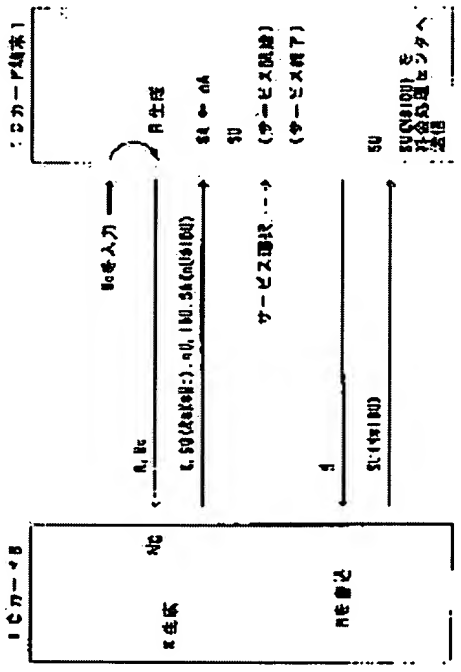
(51)Int.Cl. G06K 17/00
G06F 9/06
G06K 19/073

(21)Application number : 04-249293
(22)Date of filing : 18.09.1992

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MUTA TOSHIYASU
ISHIGURO GINYA
SAKIDA KAZUTAKA
MIYAGUCHI SHOJI
OKAMOTO TATSUAKI
FUJIOKA ATSUSHI

(54) IC CREDIT CARD SYSTEM

(57)Abstract:
PURPOSE: To make it unnecessary to access a center during the supply of service, and in addition, to improve safety.
CONSTITUTION: When a user inserts an IC card 6 into a terminal 1, and inputs a pass word Nc, a random number R is generated at the terminal 1, and the IC card 6 receives this, and when it coincides with the stored password, it generates the random number X, and produces a digital signature SU, and sends a stored digital signature SA of a card issuer corresponding to card device information IDU and the opening key nU of the card and these to the terminal 1. The terminal 1 verifies reception by using the stored opening key nA, and if it is correct, it makes user service start, and the terminal 1 transmits service information M such as a service charge and a date, etc., to the IC card 6. The IC card 6 stores this M in a memory, and simultaneously, it produces the digital signature SU, and sends it to the terminal 1. The terminal 1 verifies this, and if it is correct, it stores it in the memory, and it transmits the stored M service information etc., to the center at every definite period or every time data becomes some definite quantity.



LEGAL STATUS

[Date of request for examination] 14.10.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－103425

(43)公開日　平成６年(1994)４月15日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｋ　17/00		Ｔ　7459－5Ｌ		
Ｇ０６Ｆ　9/06	４５０　Ｂ	9367－5Ｂ		
Ｇ０６Ｋ　19/073				
		8623－5Ｌ	Ｇ０６Ｋ　19/00	Ｐ

審査請求　未請求　請求項の数２(全　９　頁)

(21)出願番号　特願平4－249293

(22)出願日　平成４年(1992)９月18日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　牟田　敏保
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　石黒　銀矢
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　崎田　一貴
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　草野　卓

最終頁に続く

(54)【発明の名称】　ＩＣクレジットカードシステム

(57)【要約】　(修正有)
【目的】　サービス提供中にセンタにアクセスする必要がなく、かつ安全性が極めて高い。
【構成】　利用者がＩＣカードを端末に挿入してパスワードＮｃを入力すると、端末に乱数Ｒを生成して、ＩＣカードへ送信する。ＩＣカードは受信して記憶してあるパスワードと一致すると、乱数Ｘを生成し、デジタル署名ＳＵを作成し、記憶してある、カード装置情報ＩＤＵとカードの公開鍵ｎＵに対するカード発行者のデジタル署名ＳＡと、これらとを端末へ送信する。端末は記憶してある公開鍵ｎＡを用いて受信を検証し、正しければ利用者サービスを開始させ、端末はサービス料金、日時などのサービス情報ＭをＩＣカードへ送信する。ＩＣカードはそのＭをメモリに記憶すると共に、デジタル署名ＳＵを作り、これを端末へ送信する。端末はこれを検証し、正しければメモリに記憶し、一定期間ごと、あるいは一定データ量になるごとに、記憶してあるＭサービス情報などをセンタへ送信する。

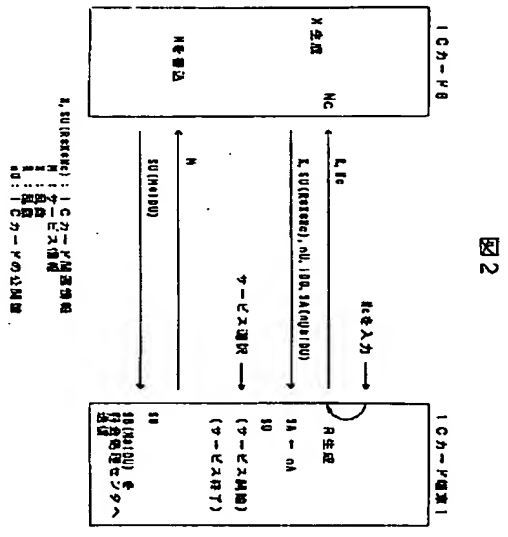


図２

1

【特許請求の範囲】

【請求項１】　乱数Ｘを発生する手段、ＩＣカード端末から受信した乱数Ｒ及び前記Ｘを含む情報に対するＩＣカードのデジタル署名ＳＵを作成する手段、ＩＣカードの公開鍵ｎＵ、ＩＣカード特定情報ＩＤＵを含む情報に対するＩＣカード発行者のデジタル署名ＳＡ、前記Ｘ、前記ＳＵ、前記ｎＵ、前記ＩＤＵをＩＣカード端末へ送信する手段、ＩＣカード端末から受信したサービス料金、サービス条件等のサービス情報Ｍと前記ＩＤＵを含む情報に対するＩＣカードのデジタル署名ＳＵを作成する手段、そのＳＵをＩＣカード端末へ送信する手段を持つＩＣカードと、

前記ＳＵ及びＳＡを受信し検証する手段、サービス終了後前記Ｍを作成し、ＩＣカードへ送信する手段、及び前記ＳＵを受信する手段を持つＩＣカード端末とより成るＩＣクレジットカードシステム。

【請求項２】　利用者が入力したパスワードをＩＣカードへ送信する手段を前記ＩＣカード端末に含み、ＩＣカード端末から受信したパスワードを予めメモリに記録してあるパスワードと比較、検証する手段を前記ＩＣカードに含むことを特徴とする請求項１記載のＩＣクレジットカードシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、予め識別番号などをセンタに登録してあるＩＣカードをＩＣカード端末へ利用者が挿入することによりサービスが提供されるＩＣクレジットカードシステムに関し、特に極めてセキュリティ（安全性）が高く、サービス提供中にはセンタにアクセスする必要のないＩＣクレジットカードシステムを得ようとするものである。

【０００２】

【従来の技術】従来、この種のシステムは、ＩＣカードとＩＣカード端末が同じ暗号方式で、同じ秘密鍵を持ち、互いに正しいＩＣカード、ＩＣカード端末であることを認証し、入力されたパスワードをＩＣカード中のパスワードと照合し、ＩＣカードからのＩＣカード識別番号をＩＣカード端末からＩＣカードに関する識別番号などのデータベースを持つセンタへ送信し、センタで検証後、検証結果をＩＣカード端末へ送信し、ＩＣカード端末で結果が良好の場合はサービスを開始する方法がとられていた。あるいは、ＩＣカードとセンタが直接、同じ秘密鍵による互いの認証を行う方法があった。

【０００３】

【発明が解決しようとする課題】従来のいずれの方法も、サービス提供前あるいは提供中に、センタとＩＣカード端末が通信する必要があり、オンラインで検証するためセンタ設備が大規模になったり、通信料がサービスの他に加わったりする欠点があった。また、センタやＩＣカードにサービスの履歴を残すことができるが、その

2

内容が不正に書込まれたものでないことを証明するのは困難であった。

【０００４】一方、文書に対し捺印するように、デジタル情報を発信した人が確かにその情報を発信し、認めたものであることを証明できるデジタル署名技術が例えば、ＮＴＴ、Ｒ＆Ｄ　Ｖｏｌ．４０，Ｎｏ．５，１９９１，ｐｐ６８７～６８６、「高速ディジタル署名方式ＥＳＩＧＮ」に示されるように確立されている。デジタル署名によれば、文書Ｍと秘密キーＫを用い、署名生成関数により作成したデジタル署名Ｓを作成し、相手にこの署名Ｓと文書Ｍを送信し、相手は送信された文書Ｍ、署名Ｓと、公開キーＵを用い、署名検証関数により確かに秘密キーＫを持つ人による文書であるか否かを検証でき、秘密キーＫを持つ人はその事実を否定できない。また、文書を一部変更しても、検証結果は不正と判定される。これらデジタル署名機能はＥＳＩＧＮと呼ばれるアルゴリズムを用いれば、ＩＣカードに実装可能なプログラム規模で実用的処理時間に収まることが、前記文献に示されている。

【０００５】この発明の目的は前記デジタル署名を利用して、サービス提供中にセンタにアクセスする必要がなく、かつ極めて安全性が高いＩＣクレジットカードシステムを提供することにある。秘密鍵Ｋを用いた文書Ｍと文書Ｎに対するデジタル署名をＳ（Ｍ＊Ｎ）と以下表記する。

【０００６】

【課題を解決するための手段】請求項１の発明によれば、乱数Ｘを発生する手段、ＩＣカード端末から受信した乱数Ｒ及び前記Ｘを含む情報に対するＩＣカードのデジタル署名ＳＵを作成する手段、ＩＣカードの公開鍵ｎＵ、ＩＣカード特定情報ＩＤＵを含む情報に対するＩＣカード発行者のデジタル署名ＳＡ、前記ＳＵ、前記Ｘ、前記ｎＵ、前記ＩＤＵをＩＣカード端末へ送信する手段、ＩＣカード端末から受信したサービス料金、サービス条件等のサービス情報Ｍを前記ＩＤＵを含む情報に対するＩＣカードのデジタル署名ＳＵを作成する手段、そのＳＵをＩＣカード端末へ送信する手段を持つＩＣカードと、前記ＳＵ及びＳＡを受信し検証する手段、サービス終了後前記Ｍを作成し、ＩＣカードへ送信する手段、及び前記ＳＵを受信する手段を持つＩＣカード端末とよりＩＣクレジットカードシステムが構成される。

【０００７】

【作用】このように構成されているから、発行者のデジタル署名付きのＩＣカードを特定する情報がＩＣカード端末で、検証できるので、ＩＣカードに関するデータベースを持つセンタへサービス利用前にアクセスする必要がなく、不正なＩＣカードによるサービス利用が排除できると共に、支払うべきサービス料金や、トラブルとなった時や利用者が参考とするための使用履歴などのサービス情報にそのＩＣカードのデジタル署名を施して、Ｉ

Ｃカード端末へ送信し、ＩＣカード端末は前記デジタル署名付きサービス情報を別途料金センタへ送信することにより、ＩＣカードのデジタル署名付きのサービス情報がセンタに記録されるためにトラブル発生時には証拠として使用できる。

【０００８】

【実施例】次に図を参照してこの発明の実施例を説明する。図１にこの発明のシステム構成例を示す。ＩＣカード６はあらかじめ図示していない発行機によって発行され、ＩＣカード特定情報（ＩＤＵ）及びその特定情報に対するＩＣカード発行者のデジタル署名（ＳＡ（ｎＵ＊ＩＤＵ））がＥＥＰＲＯＭなどのメモリに記録されている。ここで、ｎＵはＩＣカード６によるデジタル署名ＳＵを検証するための公開鍵である。またＩＣカード６にはあらかじめパスワードＮｃが記録されている。ＩＣカード６を特定する情報は料金処理センタ４に登録され、サービスを受けようとする時に、利用者がＩＣカード６をＩＣカード端末１あるいは２に挿入して、サービスを受ける。そのサービスを受けた後に、そのサービスについて料金処理センタ４でＩＣカード別に料金処理が行われる。図１は通信網３を介して相手電話機５への通信サービスを受ける場合を示している。

【０００９】図２は、この発明におけるＩＣカード６とＩＣカード端末１との間の情報の処理手順を示し、図３に、ＩＣカード端末１の内部構成例を示し、図４に、ＩＣカード６の内部構成例をそれぞれ示す。ＩＣカード端末１は挿入されたＩＣカード６に対する情報の読み出し、書き込みを行うＩＣカードリードライタ部１１と、キーボードのような操作入力部１２と、表示部１３と、各部を制御する制御部１４と、通信網３との通信を行う通信処理部１５とよりなる。ＩＣカード６においてはその処理手順、方法等のプログラムがＲＯＭ６１に記憶され、ＣＰＵ６３がワークエリアとしてＲＡＭ６２を利用してすべての制御を行い、ＩＣカード特定情報ＩＤＵ、ＩＣカード発行者のデジタル署名ＳＡなどがＥＥＰＲＯＭ６４に記憶され、通信部６５は接点６６を介してＩＣカード端末１のＩＣカードリーダライタ部１１との通信を行う。

【００１０】以下、この発明によるＩＣクレジットカードシステムの動作を図を用いて説明する。ＩＣカード６をＩＣカード端末１のＩＣカードリーダライタ部１１へ挿入すると、ＩＣカード端末１は表示部１３にパスワードＮｃを入力するように利用者へガイダンス（表示）する。

【００１１】利用者が操作入力部１２よりパスワードＮｃを入力すると、そのパスワードＮｃとＩＣカード端末１で生成した乱数ＲとをＩＣカード６へ送信する。ＩＣカード６ではそのＮｃとＲを受信後、その受信したパスワードＮｃとあらかじめメモリに記憶してあるパスワードとを比較し、一致した場合は乱数Ｘを生成し、あらかじめ発行時にＩＣカード６のＥＥＰＲＯＭ６４に記憶されているＩＣカードのデジタル署名作成用秘密鍵を用いて、Ｒ、ＸとＮｃに対するデジタル署名ＳＵ（Ｒ＊Ｘ＊Ｎｃ）を作成し、ＩＣカード関連情報即ち、乱数Ｘとデジタル署名ＳＵ（Ｒ＊Ｘ＊Ｎｃ）と、ＥＥＰＲＯＭ６４に記憶しているＩＣカードのデジタル署名検証用公開鍵ｎＵ、ＩＣカード特定情報ＩＤＵおよび、ｎＵとＩＤＵに対するＩＣカード発行者のデジタル署名ＳＡ（ｎＵ＊ＩＤＵ）を共にＩＣカード端末１へ送信する。

【００１２】ＩＣカード端末１ではＩＣカード端末設置時などあらかじめ制御部１４に設定されてあるＩＣカード発行者のデジタル署名用公開鍵ｎＡを用いてデジタル署名ＳＡを検証後、正しければ受信したｎＵを用いてデジタル署名ＳＵを検証し、正しければ、サービス選択を行うように表示部１３へガイダンスする。クレジット通話の場合は、利用者が相手電話機５のダイヤルを操作入力部１２から入力し、通信網３を介して相手電話機５と通話が開始される。その通話が終了すると、サービス料金、日時、端末識別番号、サービスアクセス先等の問題が発生した時の参考となる情報や、利用者が後程確認したい情報であるサービス情報ＭをＩＣカード６へ送信する。ＩＣカード６ではサービス情報ＭをＥＥＰＲＯＭ６４へ記憶し、さらにサービス情報ＭとＩＣカード特定情報ＩＤＵに対してＩＣカードのデジタル署名ＳＵを施し、そのデジタル署名ＳＵ（Ｍ＊ＩＤＵ）をＩＣカード端末１へ送信する。ＩＣカード端末１ではｎＵを用いてこのデジタル署名ＳＵ（Ｍ＊ＩＤＵ）を検証し、正しければ一時、制御部１４内のメモリに記憶し、例えば１週間毎に、あるいは一定量のデータが蓄積された時、または料金センタ４からポーリングがあった時に料金センタ４に通信網３を介して前記Ｍ、ＩＤＵ、ｎＵ、ＳＵ（Ｍ＊ＩＤＵ）を送信する。通信網３を介さずに携帯端末等をＩＣカード端末１に接続して前記ＳＵ（Ｍ＊ＩＤＵ）などを受信し、料金センタ４へ収集しても良い。料金センタ４ではデジタル署名ＳＵ（Ｍ＊ＩＤＵ）をさらに検証して、ＩＣカード特定情報ＩＤＵ毎にサービス情報Ｍを記録して、利用者への料金請求や、問合わせに使用する。

【００１３】ＩＣカード６及びＩＣカード端末１の各情報の送信において、両者で特定の鍵を持ち、その鍵により情報を暗号化して送信し、受信側で鍵により復号化する方法をとれば回線の盗聴などに対するセキュリティ（安全性）を高めることができる。また、ＩＣカードに有効期限情報を入れておき、ＩＣカード端末内の時計により、ＩＣカードの有効期限を検証するように構成すると紛失したＩＣカードの不正使用に対して使用制限をもうけることができる。

【００１４】さらに、ＩＣカードに初期情報を記録するカード発行機の識別番号と、その識別番号に対するＩＣカード発行者のデジタル署名、その署名の検証用公開鍵

5

をＩＣカード発行時に記録しておくことにより、ＩＣカードからＩＣカード端末へこれらの情報を送信し、ＩＣカード端末で検証することにより、正しいカード発行機で発行されたカードであることを確認することができる。

【００１５】以上の説明では落としたＩＣカードを使用できなくするため利用者がパスワードをＩＣカード端末に入力させたが、サービスによって、あるいは利用者の希望により、パスワードなしでサービスすることも考えられ、この場合は、Ｎｃがない形で図２に示した通信が行われる。さらに、以上の説明において、例えばｎＵ、ＩＤＵ、ＳＡ（ｎＵ＊ＩＤＵ）で、ｎＵ＊ＩＤＵだけではデータ量が少なく、不正される可能性がある場合など実際のシステムでは、特に必要でないデータＣを挿入して、ｎＵ、ＩＤＵ、Ｃ、ＳＡ（ｎＵ＊ＩＤＵ＊Ｃ）としてもよい。

【００１６】

6

【発明の効果】以上述べたようにこの発明によれば、ＩＣカードに発行者のデジタル署名が付いているので不正に製造されたＩＣカードはＩＣカード端末で拒否可能とすることができる。また、料金センタにＩＣカードのデジタル署名付きサービス料金等の情報を記録することが可能であるから、そのようにすればＩＣカードで利用した事を証明可能とすることができる。

【００１７】また、ＩＣカードあるいはＩＣカード端末とセンタが認証等を行うことなく、オフラインでのサービス提供が可能である。

【図面の簡単な説明】

【図１】この発明のシステム構成例を示すブロック図。

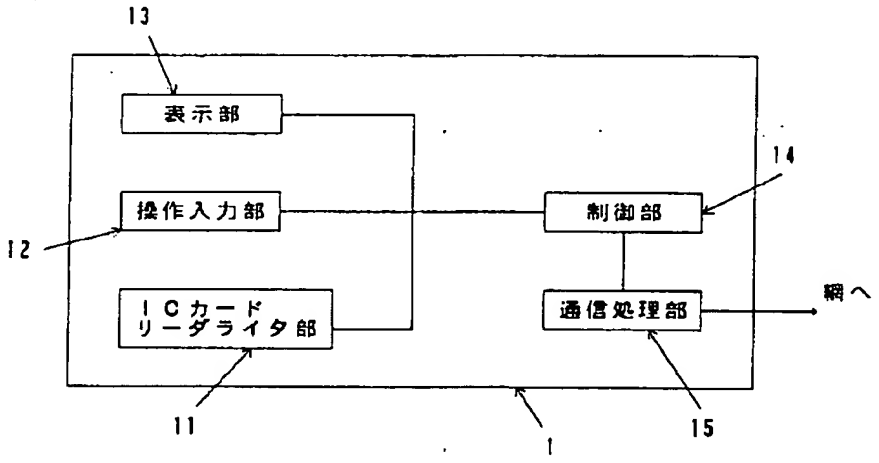
【図２】ＩＣカードとＩＣカード端末との間の情報処理、通信手順を示す図。

【図３】ＩＣカード端末の構成例を示すブロック図。

【図４】ＩＣカードの構成例を示す図。

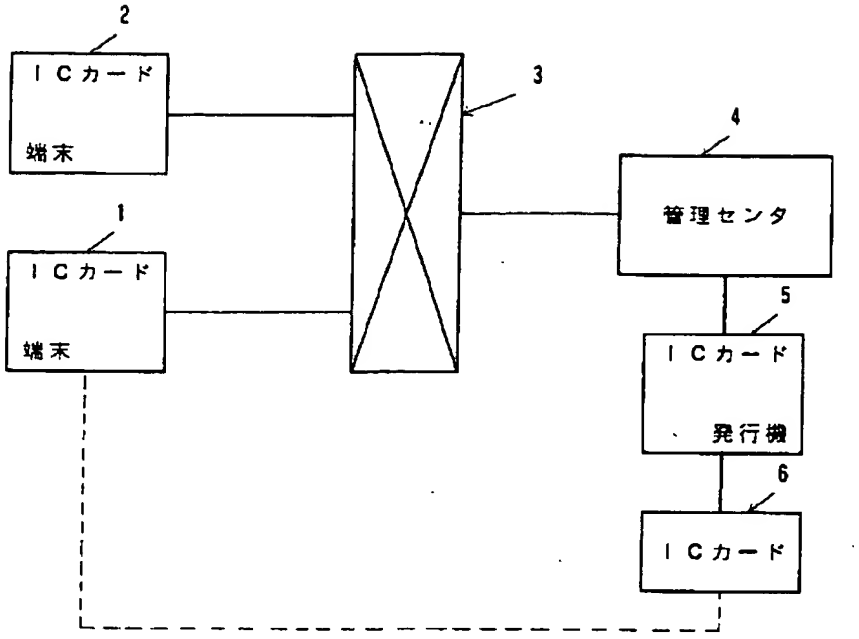
【図２】

図２



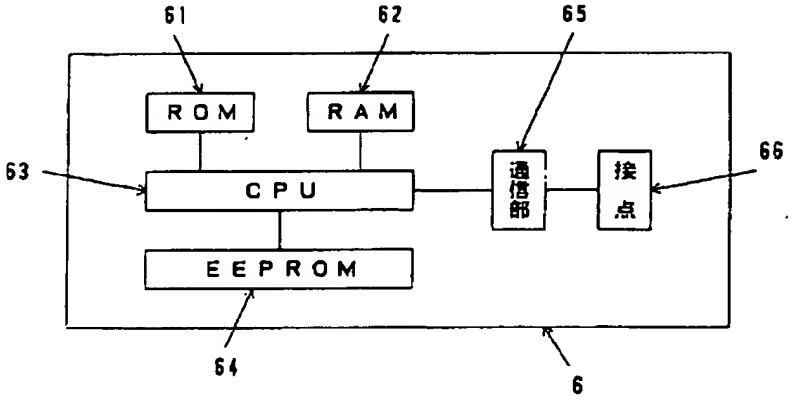
【図１】

図１



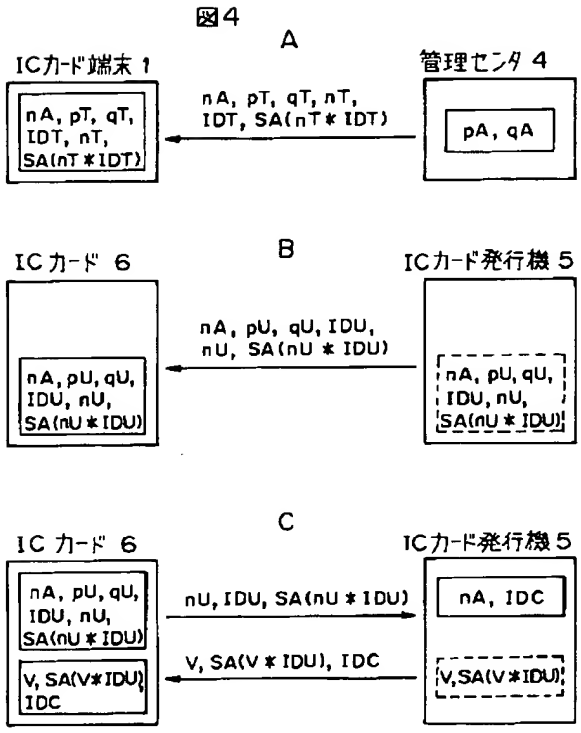
【図３】

図３



【図４】

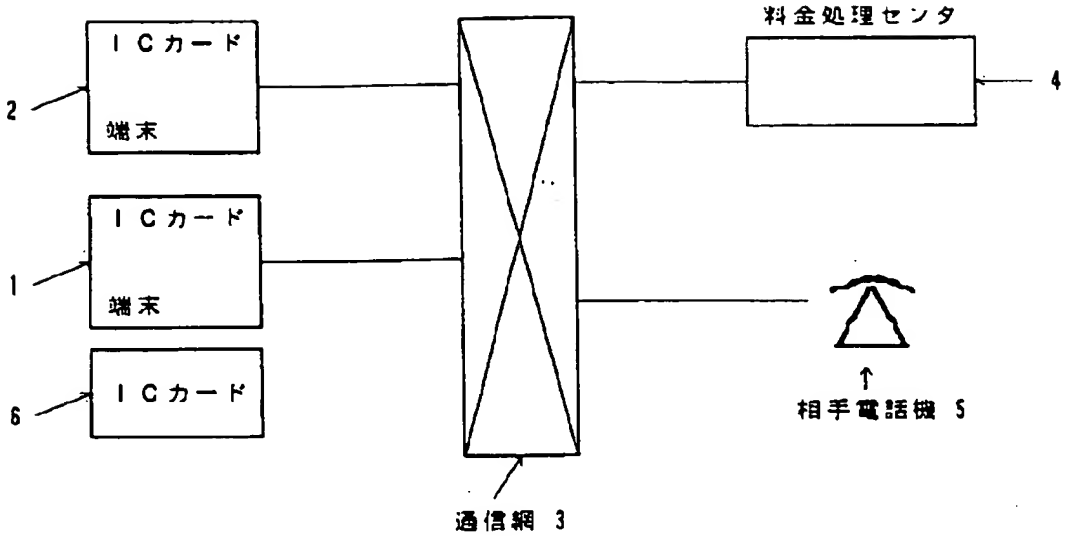
図４



【手続補正書】
【提出日】平成４年１０月２８日
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】全図
【補正方法】変更
【補正内容】

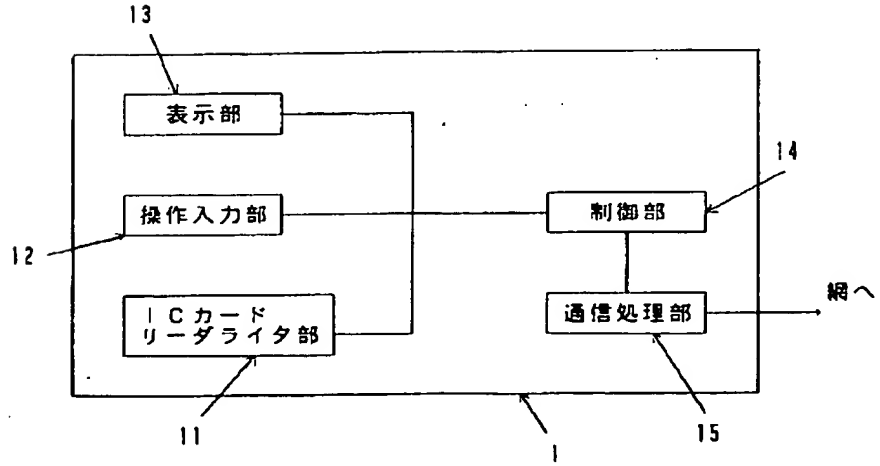
【図１】

図１


ＩＣカード
端末
2
ＩＣカード
端末
1
ＩＣカード
6
料金処理センタ
4
相手電話機 5
通信網 3

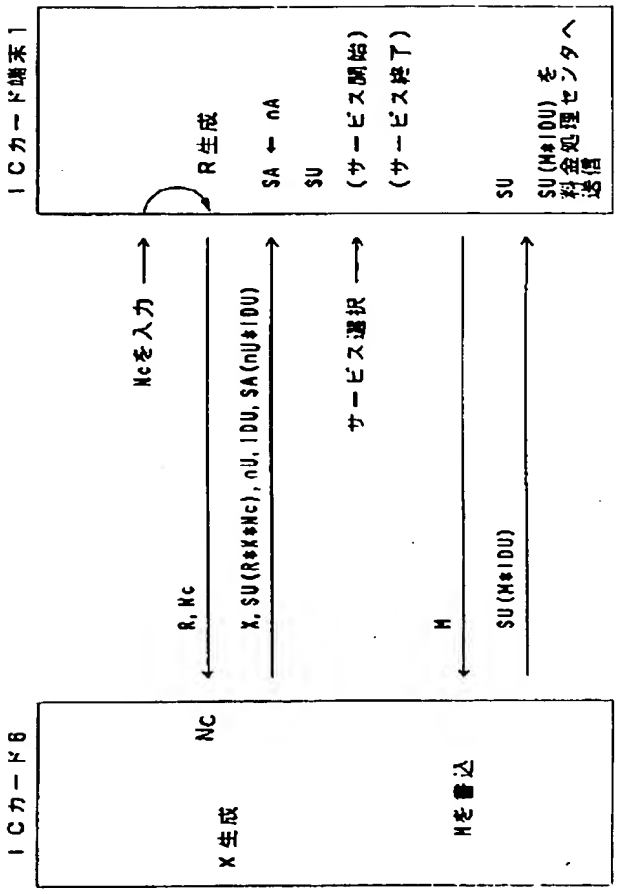
【図３】

図３


13
表示部
操作入力部
12
ＩＣカード
リーダライタ部
11
制御部
14
通信処理部
網へ
15
1

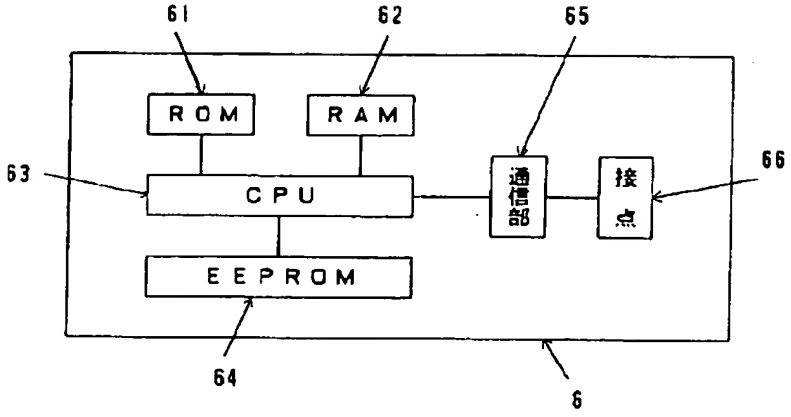
【図2】

図2


ICカード端末1
R生成
SA ← nA
SU
(サービス開始)
(サービス終了)
SU
SU(M*IDU) を
料金処理センタへ
送信
Ncを入力
サービス選択
R, Nc
X, SU(R*X*Nc), nU, IDU, SA(nU*IDU)
M
SU(M*IDU)
ICカード8
Nc
X生成
Mを書込
X, SU(R*X*Nc) : ICカード関連情報
M : サービス情報
X : 乱数
R : 乱数
nU : ICカードの公開鍵

【図４】

図４



フロントページの続き

(72)発明者　宮口　庄司
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　岡本　龍明
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　藤岡　淳
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内